Актуальные проблемы экономики и права. 2020. Т. 14, № 1
Actual Problems of Economics and Law, 2020, vol. 14, No.1
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ОТЗЫВЫ И РЕЦЕНЗИИ / RATINGS AND REVIEWS

УДК 343.3/.7:004(049.32) **DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.1.201-208**

М. А. ЕФРЕМОВА[1]

[1] *Казанский филиал Российского государственного университета правосудия, г. Казань, Россия*

РЕЦЕНЗИЯ

на монографию «Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Изд-во “Познание” Казанского инновационного университета, 2020. 300 с.»

Ефремова Марина Александровна, доктор юридических наук, профессор кафедры уголовно-правовых дисциплин, Казанский филиал Российского государственного университета правосудия
Адрес: г. Казань, ул. 2-я Азинская, 7а, тел.: +7 (843) 202-26-30
E-mail: seamaid63@gmail.com
ORCID: https://orcid.org/0000-0001-6037-6921
Web of Science Researcher ID: E-6250-2016

Цель: проведение развернутого и полного анализа монографии И. Р. Бегишева и И. И. Бикеева, которая посвящена исследованию широкого спектра вопросов, связанных с ответственностью за преступления в сфере обращения цифровой информации.
Методы: методологическую основу исследования составляет совокупность традиционных для правовых работ общенаучных и частнонаучных методов познания.
Результаты: произведен анализ основных положений и выводов, изложенных в рецензируемой монографии, касающихся юридической природы преступлений в сфере обращения цифровой информации и регламентации уголовной ответственности за их совершение, а также предложений авторов. В частности, сформулированы базовые для различных отраслей знания определения понятий цифровой информации, преступлений в сфере обращения цифровой информации и других терминов, рассмотрены проблемы «безопасной компьютерной атаки», разработаны вытекающие из авторского понимания феномена преступлений в сфере обращения цифровой информации предложения по совершенствованию ст. 137, 138, 141, 159.6, 183, 226.1, 272, 273, 274, 274.1 УК РФ, дополнению УК РФ ст. 272.1 «Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем» и ст. 273.1 «Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации».
Научная новизна: дана оценка теоретическим и прикладным аспектам противодействия преступлениям в сфере обращения цифровой информации. Сделан вывод о том, что монография вносит существенный вклад в развитие российской юридической доктрины о правовом регулировании ответственности за совершение общественно опасных деяний в сфере обращения цифровой информации.
Практическая значимость: рецензентом сделан вывод о том, что монографическое исследование И. Р. Бегишева, И. И. Бикеева имеет практико-ориентированный характер, а также может послужить импульсом для новой научной дискуссии по обозначенным в работе проблемам.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Ключевые слова: преступления в сфере обращения цифровой информации; преступления в сфере компьютерной информации; незаконный оборот специальных технических средств, предназначенных для негласного получения информации; мошенничество в сфере компьютерной информации; неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации; компьютерные преступления; противодействия преступлениям в сфере компьютерной информации; безопасность критической информационной инфраструктуры; цифровая информация; цифровые технологии; цифровая инфраструктура; цифровая экономика; преступления; уголовное право; криминология

Конфликт интересов: автором не заявлен.

Как цитировать статью: Ефремова М. А. Рецензия на монографию «Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Изд-во "Познание", 2020, 300 с.» // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 201–208. DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.1.201-208

M. A. EFREMOVA[1]

[1] *Kazan branch of the Russian State University for Justice, Kazan, Russia*

REVIEW

of the monograph «Begishev I. R., Bikeev I. I. Crimes in the sphere of digital information circulation. Kazan: Poznaniye Publishers of Kazan Innovative University, 2020, 300 p.»

Marina A. Efremova, Doctor of Law, Professor of the Department of Criminal-Legal Disciplines, Kazan branch of the Russian State University for Justice
Address: 7a 2nd Azinskaya Str., Kazan, tel.: +7 (843) 202-26-30

Objective: to conduct a detailed and comprehensive analysis of the monograph by I. R. Begishev and I. I. Bikeev devoted to the study of a wide range of issues related to liability for crimes in the field of digital information circulation.
Methods: the methodological basis of the study is a set of general and specific scientific methods of cognition traditional for works in Law.
Results: the main provisions, conclusions and the authors' suggestions set out in the reviewed monograph are analyzed, which are related to the legal nature of crimes in the sphere of digital information circulation and regulation of criminal liability for their commission. In particular, the basic definitions of digital information concepts, crimes in the sphere of digital information circulation and other terms are formulated for various branches of knowledge; the problems of "safe computer attack" are considered; based on the authors' interpretation of crimes in the sphere of digital information circulation, suggestions are made for improving Articles 137, 138, 141, 159.6, 183, 226.1, 272, 273, 274, 274.1 272.1 of the Russian Criminal Code, and complementing Article 272.1 "Acquisition or sale of legally protected digital information, knowingly obtained by criminal means" and Article 273.1 "Illegal circulation of special technical means intended for violation of digital information protection systems".
Scientific novelty: theoretical and applied aspects of countering crimes in the sphere of digital information circulation are evaluated. It is concluded that the monograph makes a significant contribution to the development of the Russian legal doctrine on the legal regulation of responsibility for committing socially dangerous acts in the sphere of digital information circulation.
Practical significance: the reviewer concluded that the monograph by I. R. Begishev and I. I. Bikeyev has a practice-oriented character, and can also serve as an impetus for a new scientific discussion on the problems identified in the study.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Keywords: Crimes in the sphere of digital information circulation; Crimes in the sphere of computer information; Illegal turnover of special technical means intended for secret obtaining of information; Fraud in the sphere of computer information; Illegal access to computer information; Creation, use and distribution of malicious computer programs; Violation of the rules of operation of means of storage, processing or transmission of computer information and information-telecommunication networks; Illegal influence on the critical information infrastructure of the Russian Federation; Computer crimes; Counteracting crimes in the field of computer information; Security of critical information infrastructure; Digital information; Digital technologies; Digital infrastructure; Digital economy; Crimes; Criminal law; Criminology

Conflict of Interest: No conflict of interest is declared by the author.

For citation: Efremova M. A. Review of the monograph "Begishev I. R., Bikeev I. I. Crimes in the sphere of digital information circulation. Kazan: Poznaniye Publishers, 2020, 300 p.", *Actual Problems of Economics and Law*, 2020, Vol. 14, No. 1, pp. 201–208 (in Russ.). DOI: http://dx.doi.org/10.21202/1993-047X.14.2020.1.201-208

Монография «Преступления в сфере обращения цифровой информации», подготовленная И. Р. Бегишевым и И. И. Бикеевым, посвящена одной из актуальных проблем, остро стоящих на современной повестке дня, – противодействию преступлениям в цифровой среде. Развитие информационных технологий существенно упростило и ускорило процесс обмена, поиска, сбора информации. Процесс информатизации, который активно начался в России в середине последнего десятилетия прошлого века, достиг своего апогея. Многие сферы жизнедеятельности человека, общества и государства трудно представить без последних достижений научно-технического прогресса, которые за последние годы в них проникли настолько глубоко, что сделали их зависимыми. Возросшая роль информации в XXI в., который называют веком информационным, как никогда актуализирует вопрос обеспечения информационной безопасности. Ведь общеизвестно, что эти, на первый взгляд, позитивные перемены, кроют в себе весьма опасный потенциал. Сегодня задачи обеспечения безопасности в цифровой среде стали одними из ключевых для большинства ведущих мировых держав. Сказанное еще раз подчеркивает актуальность темы монографии.

Теоретическая значимость монографии определяется тем, что в ней с позиции методологических основ рассмотрены проблемы уголовного права, в частности, обеспечения безопасности цифровой информации уголовно-правовыми средствами, проведено исследование базовых понятий («цифровая информация», «цифровая преступность» и т. д.) с использованием категорий других наук. Изложенное в книге обусловило высокий научный уровень рецензируемого исследования, в котором содержатся не только постановка новых вопросов, но и предложения по их разрешению. При этом авторы не уходят от полемичных проблем, а стараются разрешить их путем научной дискуссии. Такой подход позволил значительно обновить юридическую сферу научных исследований по проблемам цифровой преступности и стимулировать дальнейшие дискуссии по затронутым в работе вопросам.

Практическая значимость монографии заключается в том, что теоретические положения и выводы были трансформированы И. Р. Бегишевым и И. И. Бикеевым в сферу реализации уголовного законодательства. Сформулированные предложения по совершенствованию уголовного законодательства и практики его применения могут быть реально использованы в правотворческой и правоприменительной деятельности.

Если обратиться к структуре рецензируемой монографии, то она представляется логичной. Монография состоит из введения, трех глав, заключения, списка литературы и приложений.

Во введении обосновывается актуальность исследования, анализируется существующий научный задел по заявленной проблематике, обозначается цель исследования.

В первой главе монографии под названием «Уголовно-правовая природа преступлений в сфере цифровой информации» анализируется само понятие «цифровая информация». Авторы справедливо от-

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

мечают, что общепризнанного определения цифровой информации в правовой науке пока не выработано, а из смежных терминов наиболее часто используется термин «компьютерная информация» (с. 18). Для восполнения обозначенного пробела в работе предложено авторское определение понятия «цифровая информация» (с. 34).

Последовательно перейдя к исследованию преступлений в сфере обращения цифровой информации, И. Р. Бегишев и И. И. Бикеев акцентируют внимание на том, что и здесь современные научные подходы отличаются друг от друга, а нередко и противоречат друг другу. Вызывает научный интерес сформулированное в работе понятие «преступление в сфере обращения цифровой информации» (с. 49). Авторы подчеркивают, что защищаемыми свойствами цифровой информации ограниченного доступа являются ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность (с. 49).

Несомненную научную и практическую ценность имеет классификация преступлений в сфере обращения цифровой информации, к которым относятся деяния, предусмотренные ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», 159.6 «Мошенничество в сфере компьютерной информации», 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ», 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» Уголовного кодекса Российской Федерации[1] (далее – УК РФ) (с. 50).

Особое внимание авторы уделяют «феномену безопасной компьютерной атаки», предлагая ввести в научный оборот соответствующий термин [1]. Под таковым предлагается понимать состояние субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но в силу различных причин не обеспечивающих ее, в том числе при проведении в отношении нее компьютерных атак (с. 66).

Во второй главе монографии, именуемой «Преступления в сфере компьютерной информации по Уголовному кодексу Российской Федерации как виды преступлений в сфере обращения цифровой информации», подробно анализируются составы преступлений, включенных в гл. 28 УК РФ.

Авторы отмечают несовершенство используемой законодателем терминологии.

Так, подчеркивая несоответствие терминологии, используемой в диспозиции ст. 272 УК РФ современному этапу развития науки и техники, указывается на наличие существующего пробела в уголовно-правовой охране цифровой информации, а именно отсутствие уголовной ответственности за перехват охраняемой законом цифровой информации [2]. Для ликвидации образовавшегося пробела в работе предлагается установить уголовную ответственность за перехват охраняемой законом цифровой информации и внести соответствующие изменения в ст. 272 УК РФ, а в примечании к указанной статье сформулировать определение понятия «перехват цифровой информации» (с. 80).

Критическому анализу подвергнута и ст. 273 УК РФ, которая предусматривает уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ [3]. Пожалуй, трудно найти пользователя информационно-телекоммуникационной сети Интернет, который хотя бы раз не испытал на себе действия вредоносных компьютерных программ. Вредоносность программ определяется тем, что все действия производятся без уведомления пользователя, скрытно от него, а сам пользователь зачастую и не подозревает о наличии такой программы. В этом основное отличие вредоносных программ от иных, которые также могут производить копирование, уничтожение, модификацию информации. Сегодня вредоносные программы атакуют не только компьютеры, но и мобильные устройства. Более того, угрозам подвержена и потребительская бытовая техника. Видя недостатки в законодательной формулировке диспозиции указанного состава преступления, авторы предлагают меры для ее совершенствования (с. 94).

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в редакции Федерального закона от 27 декабря 2019 г. № 500-ФЗ) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Значительное внимание в монографии уделено и анализу ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ. Необходимо отметить, что в 2011 г. в нее были внесены изменения[2] – статья получила новую редакцию. Вместе с тем обе редакции статьи характеризуются тем, что она носит бланкетный характер [4]. Это означает, что при квалификации содеянного необходимо точное установление того правила, которое было нарушено. Во многом именно по указанной причине возникают сложности в правоприменительной практике. В период действия прежней редакции ст. 274 УК РФ таковая и вовсе отсутствовала из-за недостатков законодательной конструкции анализируемого состава. В этой связи многие авторы высказывались о необходимости исключения ее из УК РФ. И. Р. Бегишев и И. И. Бикеев справедливо отмечают, что для привлечения нарушителей работы информационно-телекоммуникационных устройств, их систем и сетей к уголовной ответственности по ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ требуется принять общие нормы и правила использования информационно-телекоммуникационных устройств, их систем и сетей, которые должны быть обязательными для всех (с. 98).

С 1 января 2018 г. вступила в силу ст. 274.1 УК РФ, которая устанавливает уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации[3]. В это же время начал свое действие Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[4]. Данная статья была помещена в гл. 28 «Преступления в сфере компьютерной информации» раздела IX «Преступления против общественной безопасности и общественного порядка». Следовательно, родовым объектом преступлений в сфере компьютерной информации должны выступать общественные отношения, обеспечивающие общественную безопасность. Видовым объектом данной группы деяний являются общественные отношения в сфере безопасного обращения компьютерной информации. Обеспечение безопасности критической информационной инфраструктуры Российской Федерации должно основываться на принципах и методологии обеспечения национальной безопасности [5]. И. Р. Бегишев и И. И. Бикеев отмечают, что воздействие на объекты критической информационной инфраструктуры Российской Федерации путем неправомерного доступа к цифровой информации или внедрения в них вредоносных компьютерных программ может нанести значительный ущерб национальной безопасности, а также привести к экологической катастрофе, человеческим жертвам и иным тяжким и особо тяжким последствиям (с. 104). Усматривая некоторые сходства неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации с актом кибертерроризма, авторы полагают, что понятие кибертерроризма в уголовном законе использовать не следует, оно должно применяться исключительно в криминологических целях, да и то очень осторожно, поскольку может трактоваться неоднозначно (с. 129).

Нельзя не поддержать позицию авторов по вопросу о том, что редакция ст. 274.1 УК РФ выглядит не совсем удачной и требует изменений.

В третьей главе монографии под названием «Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации», исследуются составы преступлений, совершаемых с использованием компьютерной техники и иных технических устройств, а также

[2] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 7 декабря 2011 г. (в ред. Федерального закона № 329-ФЗ от 3 июля 2016 г.) // Собрание законодательства РФ. 2011. № 50. Ст. 7362.

[3] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон № 194-ФЗ от 26 июля 2017 г. // Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4743.

[4] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4736.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

дается прогноз появления новых проявлений деяний подобного рода.

Авторами подробно проанализирован состав преступления, предусмотренного ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», которое, по их мнению, может совершаться как с использованием вредоносных компьютерных программ, так и с нарушением систем защиты цифровой информации [6]. И. Р. Бегишев и И. И. Бикеев обосновывают, что деяние, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, относится к преступлениям в сфере обращения цифровой информации и совершается с ее использованием, поэтому предлагают указанную статью назвать «Мошенничество с использованием цифровой информации» (с. 177).

Подробный анализ ст. 138.1 УК РФ, которая предусматривает ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации, позволил авторам выявить ее несовершенства и предложить ряд изменений [7]. Так, вместо термина «специальные технические средства, предназначенные для негласного получения информации» предложено использовать в УК РФ более точный и недвусмысленный термин «технические средства негласного получения информации» (с. 190).

Авторы обоснованно обращают внимание на тот факт, что отечественный законодатель не в полной мере учел общественную опасность неправомерного обращения с техническими средствами негласного получения информации [8]. Вызывает интерес и заслуживает поддержки их предложение установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 «Нарушение неприкосновенности частной жизни», ч. 2 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ч. 2 ст. 141 «Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий» и ч. 3 ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ (с. 196).

Весьма оправданной требованиями времени выглядит инициатива авторов о принятии отдельного федерального закона «О специальных технических средствах», который определял бы правила оборота таких средств, содержание используемых понятий, перечень субъектов, которым разрешено использовать указанные средства, установить порядок их применения и т. д. (с. 197).

Специальные технические средства могут быть использованы не только для негласного получения информации, но и для нарушения систем защиты цифровой информации, что, безусловно, представляет повышенную общественную опасность, однако действующий УК РФ не содержит отдельной нормы, предусматривающей ответственность за подобного рода деяние [9]. И. Р. Бегишев и И. И. Бикеев предлагают включить в УК РФ ст. 273.1 «Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации», что позволит восполнить возникший пробел в законе (с. 208).

Авторы отмечают, что цифровая информация, полученная незаконным путем, может быть передана третьим лицам для последующего распоряжения таковой. Кроме того, на практике нередки случаи, когда лицо стремится приобрести такую информацию с целью совершения иных неправомерных действий [10]. Действительно, УК РФ уже содержит ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем», однако в этой норме нет указания на цифровую информацию, что не позволяет привлечь лицо к ответственности, в случае если деяние совершено в отношении цифровой информации [11–14]. Ввиду изложенного своевременным и востребованным видится предложение авторов о криминализации такого деяния путем включения в УК РФ ст. 272.1, предусматривающей ответственность за приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем (с. 225).

Заключение содержит основные выводы авторов по вопросам, затронутым в рецензируемой монографии, а также предложение к научной дискуссии по проблемам цифровой преступности, которая могла бы развернуться на страницах ведущих рецензируемых научных изданий.

Характеризуя монографию И. Р. Бегишева и И. И. Бикеева в целом, следует отметить, что исследование выполнено на высоком теоретико-методологическом уровне. Множество выводов и положений,

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

изложенных в ней, действительно представляют научный интерес, так как соединяют в себе теоретико-прикладные аспекты.

При этом необходимо отметить, что книга базируется на солидном количестве ранее проведенных ее авторами исследований, результаты которых опубликованы в ведущих рецензируемых научных изданиях.

Завершая рецензию, необходимо подчеркнуть, что монография на тему «Преступления в сфере обращения цифровой информации» вносит существенный вклад в развитие российской юридической доктрины о правовом регулировании ответственности за совершение общественно опасных деяний в сфере обращения цифровой информации. Значительная часть выводов авторов монографии направлена на развитие правоприменительной практики по обеспечению безопасного оборота цифровой информации.

Последующие исследования по проблемам уголовно-правовой охраны цифровой информации, сама практика применения уголовного закона выявят новые пробелы и недостатки, что позволит продолжить новый научный поиск. Однако на сегодняшний день монография «Преступления в сфере обращения цифровой информации», подготовленная И. Р. Бегишевым и И. И. Бикеевым, является одной из немногих, где в полной мере систематизированы и отражены проблемы противодействия преступлениям в сфере обращения цифровой информации и предложены пути их решения.

Список литературы

1. Бегишев И. Р. Синдром безопасной атаки: юридико-психологический феномен // Юридическая психология. 2018. № 2. С. 27–30.

2. Бегишев И. Р. Перехват охраняемой законом цифровой информации: уголовно-правовые аспекты // Информационная безопасность регионов. 2011. № 1. С. 78–81.

3. Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3. С. 218–221.

4. Бегишев И. Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УрФО. Безопасность в информационной сфере. 2012. № 1. С. 15–18.

5. Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

6. Бегишев И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3. С. 112–117.

7. Бегишев И. Р. Правовые аспекты безопасности информационного общества // Информационное общество. 2011. № 4. С. 54–59.

8. Бегишев И. Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации // Следователь. 2010. № 5. С. 2–4.

9. Бегишев И. Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект // Информация и безопасность. 2010. № 2. С. 255–258.

10. Бегишев И. Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем // Безопасность информационных технологий. 2010. № 1. С. 43–44.

11. Бегишев И. Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем // Актуальные проблемы экономики и права. 2010. № 1. С. 123–126.

12. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. … канд. юрид. наук. Казань, 2017. 31 с.

13. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук. Казань, 2017. 204 с.

14. Бикеев И. И. Материальные объекты повышенной опасности в российском уголовном праве: общие и специальные вопросы. Казань: Изд-во «Познание», 2007. 272 с.

15. Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Изд-во «Познание» Казанского инновационного университета, 2020, 300 с.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

References

1. Begishev I. R. Syndrome of a safe attack: legal-psychological phenomenon, *Yuridicheskaya psikhologiya*, 2018, No. 2, pp. 27–30 (in Russ.).

2. Begishev I. R. Interception of digital information protected by law: criminal-legal aspects, *Informatsionnaya bezopasnost' regionov*, 2011, No. 1, pp. 78–81 (in Russ.).

3. Begishev I. R. Creating, using and distributing harmful computer software, *Problemy prava*, 2012, No. 3, pp. 218–221 (in Russ.).

4. Begishev I. R. Liability for violating the rules of exploitation of means of storing, processing or transmitting computer information and information-telecommunication networks, *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2012, No. 1, pp. 15–18 (in Russ.).

5. Begishev I. R. Safety of critical information infrastructure of the Russian Federation, *Bezopasnost' biznesa*, 2019, No. 1, pp. 27–32 (in Russ.).

6. Begishev I. R. Some issues of counteracting fraud in the sphere of computer information, *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 2016, No. 3, pp. 112–117 (in Russ.).

7. Begishev I. R. Legal aspects of safety of information society, *Informatsionnoe obshchestvo*, 2011, No. 4, pp. 54–59 (in Russ.).

8. Begishev I. R. Issues of criminal liability for using special technical means intended for undercover obtaining of information, *Sledovatel'*, 2010, No. 5, pp. 2–4 (in Russ.).

9. Begishev I. R. Manufacturing, marketing and purchasing of special technical means aimed at violating the systems of digital information protection: legal aspect, *Informatsiya i bezopasnost'*, 2010, No. 2, pp. 255–258 (in Russ.).

10. Begishev I. R. Issues of liability for illegal actions with information knowingly obtained with criminal means, *Bezopasnost' informatsionnykh tekhnologii*, 2010, No. 1, pp. 43–44 (in Russ.).

11. Begishev I. R. Criminal liability for purchasing or marketing of digital and documented information knowingly obtained with criminal means, *Actual Problems of Economics and Law*, 2010, No. 1, pp. 123–126 (in Russ.).

12. Begishev I. R. *Notion and types of crimes in the sphere of digital information circulation*, abstract of PhD (Law) thesis, Kazan, 2017, 31 p. (in Russ.)

13. Begishev I. R. *Notion and types of crimes in the sphere of digital information circulation*, PhD (Law) thesis, Kazan, 2017, 204 p. (in Russ.)

14. Bikeev I. I. *Highly hazardous material objects in the Russian criminal law: general and special issues*, Kazan, Poznanie, 2007, 272 p. (in Russ.).

15. Begishev I. R., Bikeev I. I. *Crimes in the sphere of digital information circulation*. Kazan: Poznaniye Publishers of Kazan Innovative University, 2020, 300 p. (in Russ.).

Дата поступления / Received 13.01.2020
Дата принятия в печать / Accepted 20.02.2020
Дата онлайн-размещения / Available online 25.03.2020